

JP 01/772

EU

PCT/JP01/00772

02.02.01

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

#4

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

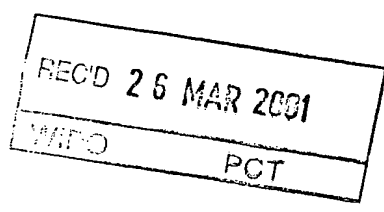
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

2000年 7月11日

出 願 番 号
Application Number:

特願2000-209674



出 願 人
Applicant (s):

ソニー株式会社

091937797

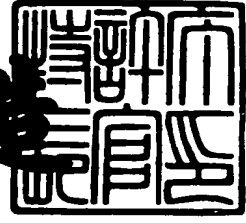
PRIORITY
DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2001年 3月 2日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3015161

【書類名】 特許願

【整理番号】 0000199003

【提出日】 平成12年 7月11日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 佐竹 清

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 金巻 裕史

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100094053

 【弁理士】

 【氏名又は名称】 佐藤 隆久

【手数料の表示】

 【予納台帳番号】 014890

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9707389

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証装置、認証システムおよびその方法

【特許請求の範囲】

【請求項 1】

第 1 の取り引き者に関する情報を保持し、第 2 の取り引き者に関する情報を保持する他の認証装置との間で通信を行いながらネットワークを介して行われる前記第 1 の取り引き者と前記第 2 の取り引き者との間の取り引きに関する認証を行う認証装置であって、

前記取り引き内容を示す情報と前記第 2 の取り引き者を特定する情報とを含む前記第 1 の取り引き者からの第 1 の要求に応じて、前記第 2 の取り引き者を特定する情報を含む第 2 の要求を前記第 2 の認証装置に送信し、前記第 2 の要求に応じた前記第 2 の認証装置による認証結果を示す第 1 の署名情報を受信し、前記第 1 の要求に含まれる前記取り引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信し、当該第 3 の要求に応じて前記第 2 の取り引き者が使用する装置から所定の応答を受ける送受信手段と、

前記所定の応答を受けた場合に、前記取り引きの履歴を記憶する記憶手段と、

前記所定の応答を受けた場合に、前記送受信手段を介して前記第 1 の取り引き者が使用する装置に送信される第 2 の署名情報であって、前記取り引きの正当性の認証結果を示す第 2 の署名情報を作成する署名作成手段と

を有する認証装置。

【請求項 2】

暗号化手段

をさらに有し、

前記送受信手段は、前記第 2 の取り引き者との間の通信に用いる暗号鍵を前記第 2 の要求に応じて前記他の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第 1 の署名情報とを、前記第 2 の取り引き者が使用する装置に送信する

請求項 1 に記載の認証装置。

【請求項 3】

前記送受信手段は、

前記他の認証装置が前記第 2 の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第 2 の取り引き者が使用する装置から受け、

前記記憶手段は、前記識別情報を用いて生成された前記取り引きの履歴を記憶する

請求項 1 に記載の認証装置。

【請求項 4】

前記送受信手段は、前記第 1 の要求に含まれる前記取り引き内容に関する情報のうち、前記第 1 の取り引き者の課金に係わる情報以外の情報と、前記第 1 の署名情報とを含む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信する

請求項 1 に記載の認証装置。

【請求項 5】

前記送受信手段は、前記第 1 の要求に含まれる前記取り引き内容に関する情報と、前記第 1 の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信する

請求項 1 に記載の認証装置。

【請求項 6】

前記取り引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する請求項 1 に記載の認証装置。

【請求項 7】

前記課金処理手段は、前記他の認証装置との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う

請求項 6 に記載の認証装置。

【請求項 8】

前記送受信手段は、前記第 2 の取り引き者が前記第 1 の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第 2 の取り引き者が使用する装置から、前記所定の応答を受ける

請求項 1 に記載の認証装置。

【請求項 9】

前記送受信手段は、

前記第 2 の署名情報を前記第 2 の取引引き者が使用する装置に送信する

請求項 1 に記載の認証装置。

【請求項 1 0】

ネットワークを介して少なくとも 2 者間で行われた取引引きを認証する認証方法システムにおいて、

第 1 の取引引き者に関する取引引きを認証する第 1 の認証装置と、

第 2 の取引引き者に関する取引引きを認証する第 2 の認証装置と

を有し、

前記第 1 の認証装置は、

前記取引引き内容を示す情報と前記第 2 の取引引き者を特定する情報とを含む前記第 1 の取引引き者による第 1 の要求に応じて、前記第 2 の取引引き者を特定する情報を含む第 2 の要求を前記第 2 の認証装置に送信し、前記第 2 の要求に応じた前記第 2 の認証装置による認証結果である第 1 の署名情報を受信し、前記第 1 の要求に含まれる前記取引引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を前記第 2 の取引引き者が使用する装置に送信し、当該第 3 の要求に応じて前記第 2 の取引引き者から所定の応答を受けると、前記取引引きの履歴を記憶し、前記取引引きの正当性の認証結果を示す第 2 の署名情報を前記第 1 の取引引き者に提供する

認証システム。

【請求項 1 1】

前記第 1 の認証装置は、

暗号化手段

をさらに有し、

前記送受信手段は、前記第 2 の取引引き者との間の通信に用いる暗号鍵を前記第 2 の要求に応じて前記第 2 の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取引引き内容に関する情報と前記第 1 の署名情報とを、前記第 2 の取引引き者が使用する装置に送信する

請求項 1 0 に記載の認証システム。

【請求項 1 2】

前記第 1 の認証装置の前記送受信手段は、

前記第 2 の認証装置が前記第 2 の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第 2 の取り引き者が使用する装置から受け、

前記記憶手段は、前記識別情報を用いて生成された前記取り引きの履歴を記憶する

請求項 1 0 に記載の認証システム。

【請求項 1 3】

前記第 1 の認証装置は、

前記第 2 の署名情報を前記第 2 の取り引き者に提供する

請求項 1 0 に記載の認証システム。

【請求項 1 4】

第 1 の取り引き者に関する取り引きを認証する第 1 の認証装置と、第 2 の取り引き者に関する取り引きを認証する第 2 の認証装置とを用いて、ネットワークを介して行われる前記第 1 の取り引き者と前記第 2 の取り引き者との間の取り引きに関する認証を行う認証方法であって、

前記第 1 の取り引き者から前記第 1 の認証装置に、前記取り引き内容を示す情報と前記第 2 の取り引き者を特定する情報とを含む第 1 の要求を出し、

前記第 1 の要求に応じて、前記第 1 の認証装置から前記第 2 の認証装置に、前記第 2 の取り引き者を特定する情報を含む第 2 の要求を送信し、

前記第 2 の要求に応じて、前記第 2 の認証装置からの前記第 1 の認証装置に、当該第 2 の認証装置による認証結果を示す第 1 の署名情報を送信し、

前記第 1 の認証装置から前記第 2 の取り引き者が使用する装置に、前記第 1 の要求に含まれる前記取り引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を送信し、

当該第 3 の要求に応じて、前記第 2 の取り引き者が使用する装置から前記第 1 の認証装置に所定の応答を出し、

前記所定の応答に応じて、前記第 1 の認証装置は、前記取り引きの履歴を記憶

し、前記取り引きの正当性の認証結果を示す第2の署名情報を作成し、当該第2の署名情報を、前記第1の取り引き者が使用する装置に送信する

認証方法。

【請求項15】

前記第2の取り引き者との間の通信に用いる暗号鍵を前記第2の要求に応じて、前記第2の認証装置から前記第1の認証装置に送信し、

前記第1の認証装置は、前記取り引き内容に関する情報と前記第1の署名情報とを、前記暗号鍵を用いて暗号化した後に、前記第2の取り引き者が使用する装置に送信する

請求項14に記載の認証方法。

【請求項16】

前記第1の認証装置は、前記第2の認証装置が前記第2の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第2の取り引き者が使用する装置から受け、前記識別情報を用いて生成された前記取り引きの履歴を記憶する

請求項14に記載の認証方法。

【請求項17】

前記第1の要求に含まれる前記取り引き内容に関する情報のうち、前記第1の取り引き者の課金に係わる情報以外の情報と、前記第1の署名情報とを含む第3の要求を、前記第1の認証装置から前記第2の取り引き者が使用する装置に送信する

請求項14に記載の認証方法。

【請求項18】

前記第1の要求に含まれる前記取り引き内容に関する情報と、前記第1の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第3の要求を、前記第1の認証装置から前記第2の取り引き者が使用する装置に送信する

請求項14に記載の認証方法。

【請求項19】

前記第1の認証装置と前記第2の認証装置との間で、前記取り引きに関する認

証に対して行う課金の割合を決定するための処理を行う

請求項 1 4 に記載の認証方法。

【請求項 2 0】

前記第 2 の取り引き者が前記第 1 の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第 2 の取り引き者が使用する装置から前記第 1 の認証装置に、前記所定の応答を出す

請求項 1 4 に記載の認証方法。

【請求項 2 1】

前記第 1 の認証装置から前記第 2 の取り引き者が使用する装置に、前記第 2 の署名情報を送信する

請求項 1 4 に記載の認証方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、電子商取引情報を認証する認証装置、認証システムおよびその方法に関する。

【0 0 0 2】

【従来の技術】

インターネットなどのネットワークを介して商品等の販売や代金の決済を行う電子商取引が普及している。

このような電子商取引を用いて利用者が商品等を購入する場合には、例えば、利用者が店舗や各家庭に設置されたパーソナルコンピュータなどの発注者端末装置を操作して、ネットワークを介して、商品等の販売を行うサーバ装置にアクセスを行う。これにより、サーバ装置から発注者端末装置に商品の写真、特性および価格などの情報が提供され、発注者端末装置のディスプレイに表示される。利用者は、このような情報を見ながら、購入を希望する商品等を選択し、選択した商品等の発注処理を行う。発注処理は、利用者個人を認証する個人認証情報、購入を希望する商品等を指定した情報およびその決済方法等の情報を、発注者端末装置を操作して入力し、これをネットワークを介してサーバ装置に送信する。

【 0 0 0 3 】

このような電子商取引では、ネットワーク銀行などが、ネットワークを介した取引に関する決済業務を行うが、当該決済を行うに当たって、決済対象となる電子商取引の内容の正当性が認証されている必要がある。

従って、電子商取引では、このような電子商取引の内容の正当性を認証する認証装置が用いられる。当該認証装置を用いた認証業務は、ネットワーク銀行、あるいは他の信頼性のある機関が行う。

【 0 0 0 4 】

【発明が解決しようとする課題】

ところで、上述したような電子商取引が普及すると、複数に認証機関が、電子商取引の認証業務を行うことになる。

この場合に、同じ電子商取引に参加した利用者が、それぞれ異なる認証機関と契約をしている場合に、どのようにして当該電子商取引の正当性を認証するかが課題となる。

この場合に、同じ電子商取引に参加した利用者が契約した複数の認証機関で、利用者の情報を共有することで、上述した課題に対処できるが、利用者の個人情報、他の機関に漏れてしまうという問題がある。

【 0 0 0 5 】

本発明は上述した従来技術の問題点に鑑みてなされ、異なる認証機関と契約した利用者相互間の取引の認証を、利用者の個人情報を他の認証機関に提供することなく、高い信頼性で行うことができる認証装置、認証システムおよびその方法を提供することを目的とする。

【 0 0 0 6 】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第1の発明の認証装置は、第1の取引者に関する情報を保持し、第2の取引者に関する情報を保持する他の認証装置との間で通信を行いながらネットワークを介して行われる前記第1の取引者と前記第2の取引者との間の取引に関する認証を行う認証装置であって、前記取引内容を示す情報と前記第2

の取り引き者を特定する情報とを含む前記第 1 の取り引き者からの第 1 の要求に応じて、前記第 2 の取り引き者を特定する情報を含む第 2 の要求を前記第 2 の認証装置に送信し、前記第 2 の要求に応じた前記第 2 の認証装置による認証結果を示す第 1 の署名情報を受信し、前記第 1 の要求に含まれる前記取り引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信し、当該第 3 の要求に応じて前記第 2 の取り引き者が使用する装置から所定の応答を受ける送受信手段と、前記所定の応答を受けた場合に、前記取り引きの履歴を記憶する記憶手段と、前記所定の応答を受けた場合に、前記送受信手段を介して前記第 1 の取り引き者が使用する装置に送信される第 2 の署名情報であって、前記取り引きの正当性の認証結果を示す第 2 の署名情報を作成する署名作成手段とを有する。

【 0 0 0 7 】

第 1 の発明の認証装置の作用は以下になる。

送受信手段、前記取り引き内容を示す情報と前記第 2 の取り引き者を特定する情報とを含む前記第 1 の取り引き者からの第 1 の要求を受ける。

そして、当該第 2 の要求に応じて、前記第 2 の取り引き者を特定する情報を含む第 2 の要求が、前記送受信手段から前記第 2 の認証装置に送信される。

次に、送受信手段は、前記第 2 の要求に応じた第 1 の署名情報を前記第 2 の認証装置から受信する。

次に、前記第 1 の要求に含まれる前記取り引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を、前記送受信手段から前記第 2 の取り引き者が使用する装置に送信する。

次に、送受信手段は、当該第 3 の要求に応じて前記第 2 の取り引き者が使用する装置から所定の応答を受ける。

前記送受信手段が前記所定の応答を受けると、記憶手段に、前記取り引きの履歴が記憶される。

また、前記送受信手段が前記所定の応答を受けると、署名作成手段によって、前記取り引きの正当性を認証する第 2 の署名情報が作成され、当該第 2 の署名情報が、前記送受信手段を介して前記第 1 の取り引き者が使用する装置に送信され

る。

【 0 0 0 8 】

また、第 1 の発明の認証装置は、好ましくは、暗号化手段をさらに有し、前記送受信手段は、前記第 2 の取り引き者との間の通信に用いる暗号鍵を前記第 2 の要求に応じて前記他の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第 1 の署名情報とを、前記第 2 の取り引き者が使用する装置に送信する。

【 0 0 0 9 】

また、第 1 の発明の認証装置は、好ましくは、前記送受信手段は、前記他の認証装置が前記第 2 の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第 2 の取り引き者が使用する装置から受け、前記記憶手段は、前記識別情報を用いて生成された前記取り引きの履歴を記憶する。

【 0 0 1 0 】

また、第 1 の発明の認証装置は、好ましくは、前記送受信手段は、前記第 1 の要求に含まれる前記取り引き内容に関する情報のうち、前記第 1 の取り引き者の課金に係わる情報以外の情報と、前記第 1 の署名情報とを含む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信する。

【 0 0 1 1 】

また、第 1 の発明の認証装置は、好ましくは、前記送受信手段は、前記第 1 の要求に含まれる前記取り引き内容に関する情報と、前記第 1 の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信する。

【 0 0 1 2 】

また、第 1 の発明の認証装置は、好ましくは、前記取り引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する。

【 0 0 1 3 】

また、第 1 の発明の認証装置は、好ましくは、前記課金処理手段は、前記他の認証装置との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う。

【 0 0 1 4 】

また、第 1 の発明の認証装置は、好ましくは、前記送受信手段は、前記第 2 の取り引き者が前記第 1 の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第 2 の取り引き者が使用する装置から、前記所定の応答を受ける。

【 0 0 1 5 】

また、第 2 の発明の認証システムは、ネットワークを介して少なくとも 2 者間で行われた取り引きを認証する認証方法システムであって、第 1 の取り引き者に関する取り引きを認証する第 1 の認証装置と、第 2 の取り引き者に関する取り引きを認証する第 2 の認証装置とを有し、前記第 1 の認証装置は、前記取り引き内容を示す情報と前記第 2 の取り引き者を特定する情報とを含む前記第 1 の取り引き者による第 1 の要求に応じて、前記第 2 の取り引き者を特定する情報を含む第 2 の要求を前記第 2 の認証装置に送信し、前記第 2 の要求に応じた前記第 2 の認証装置からの第 1 の署名情報を受信し、前記第 1 の要求に含まれる前記取り引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信し、当該第 3 の要求に応じて前記第 2 の取り引き者から所定の応答を受けると、前記取り引きの履歴を記憶し、前記取り引きの正当性を認証する第 2 の署名情報を前記第 1 の取り引き者に提供する。

【 0 0 1 6 】

また、第 2 の発明の認証システムは、前記第 1 の認証装置は、暗号化手段をさらに有し、前記送受信手段は、前記第 2 の取り引き者との間の通信に用いる暗号鍵を前記第 2 の要求に応じて前記第 2 の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第 1 の署名情報とを、前記第 2 の取り引き者が使用する装置に送信する。

【 0 0 1 7 】

また、第 3 の発明の認証方法は、第 1 の取り引き者に関する取り引きを認証する第 1 の認証装置と、第 2 の取り引き者に関する取り引きを認証する第 2 の認証装置とを用いて、ネットワークを介して行われる前記第 1 の取り引き者と前記第 2 の取り引き者との間の取り引きに関する認証を行う認証方法であって、前記第

1の取引引き者から前記第1の認証装置に、前記取引引き内容を示す情報と前記第2の取引引き者を特定する情報とを含む第1の要求を出し、前記第1の要求に応じて、前記第1の認証装置から前記第2の認証装置に、前記第2の取引引き者を特定する情報を含む第2の要求を送信し、前記第2の要求に応じて、前記第2の認証装置からの前記第1の認証装置に、当該第2の認証装置による認証結果を示す第1の署名情報を送信し、前記第1の認証装置から前記第2の取引引き者が使用する装置に、前記第1の要求に含まれる前記取引引き内容に関する情報と前記第1の署名情報とを含む第3の要求を送信し、当該第3の要求に応じて、前記第2の取引引き者が使用する装置から前記第1の認証装置に所定の応答を出し、前記所定の応答に応じて、前記第1の認証装置は、前記取引引きの履歴を記憶し、前記取引引きの正当性の認証結果を示す第2の署名情報を作成し、当該第2の署名情報を、前記第1の取引引き者が使用する装置に送信する。

【0018】

また、第3の発明の認証方法は、好ましくは、前記第2の取引引き者との間の通信に用いる暗号鍵を前記第2の要求に応じて、前記第2の認証装置から前記第1の認証装置に送信し、前記第1の認証装置は、前記取引引き内容に関する情報と前記第1の署名情報とを、前記暗号鍵を用いて暗号化した後に、前記第2の取引引き者が使用する装置に送信する。

【0019】

【発明の実施の形態】

以下、本発明の実施形態に係わるトランザクション認証システムについて説明する。

図1は、本実施形態のトランザクション認証システム1の全体構成図である。

図1に示すように、トランザクション認証システム1では、例えば、発注者31の発注者端末装置11と、受注者33の受注者端末装置15と、ネットワーク銀行40の認証装置50と、ネットワーク銀行41の認証装置51とが、インターネットなどのネットワーク（通信網）を介して接続されており、発注者31と受注者33との間のトランザクション（取引引き）の正当性を認証する。

【0020】

本実施形態では、例えば、発注者 3 1 とネットワーク銀行 4 0 との間で認証を行うことについての契約が成されており、受注者 3 3 とネットワーク銀行 4 1 との間で認証を行うことについての契約が成されている。

また、ネットワーク銀行 4 0 とネットワーク銀行 4 1 とでは、認証に関して、相互に連携する旨の相互乗り入れの契約が成されている。

【 0 0 2 1 】

本実施形態では、発注者 3 1 が本発明の第 1 の取り引き者に対応し、受注者 3 3 が本発明の第 2 の取り引き者に対応している。

また、認証装置 5 0 が、第 1 の発明の認証装置、並びに第 2 の発明および第 3 の発明の第 1 の認証装置に対応している。

また、認証装置 5 1 が、第 1 の発明の他の認証装置、並びに第 2 の発明および第 3 の発明の第 2 の認証装置に対応している。

【 0 0 2 2 】

以下、トランザクション認証システム 1 を構成する各装置について説明する。

〔発注者端末装置 1 1〕

図 2 に示すように、発注者端末装置 1 1 は、例えば、発注者 3 1 の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部 6 1、送信部 6 2、暗号化部 6 3、復号部 6 4、記憶部 6 5、制御部 6 6 および署名検証部 6 7 を有する。

なお、発注者端末装置 1 1 は、例えば、発注者 3 1 が使用する際に、発注者 3 1 の指紋等の身体的特徴から得られる情報と、予め記憶部 6 5 に予め記憶してある身体的特徴を示す情報とを比較することで、発注者 3 1 が正当な使用者であることを認証する生体認証部を有していてもよい。

【 0 0 2 3 】

受信部 6 1 は、ネットワークを介して認証装置 5 0 から情報あるいは要求を受信する。

送信部 6 2 は、ネットワークを介して認証装置 5 0 に情報あるいは要求を送信する。

また、受信部 6 1 および送信部 6 2 は、受注者 3 3 が提供する商品等の案内情

報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部 63 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 64 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 65 は、例えば、発注者 31 がネットワーク銀行 40 と契約を行うと、例えば、発注者 31 に割り当てられた秘密鍵 $K_{31,S}$ などを格納する。

制御部 66 は、発注者端末装置 11 内の各構成要素の処理を統括的に制御する。

署名検証部 67 は、例えば、認証装置 50 が作成した署名情報を、ネットワーク銀行 40 の公開鍵 $K_{40,P}$ を用いて検証する。

【0024】

〔受注者端末装置 15〕

図 3 に示すように、受注者端末装置 15 は、サイバーモール(Cyber Mall)などに店舗を出している受注者 33 が使用するサーバ装置であり、受信部 71、送信部 72、暗号化部 73、復号部 74、記憶部 75、制御部 76 および署名検証部 77 を有する。

受信部 71 は、ネットワークを介して認証装置 50、51 から情報あるいは要求を受信する。

送信部 72 は、ネットワークを介して認証装置 50、51 に情報あるいは要求を送信する。

また、受信部 71 および送信部 72 は、発注者端末装置 11 からのアクセスに応じて、例えば、記憶部 75 から読み出した受注者 33 が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置 11 に送信する。

暗号化部 73 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 74 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 75 は、例えば、受注者 33 がネットワーク銀行 41 と契約を行うと、例えば、受注者 33 に割り当てられた秘密鍵 $K_{33,S}$ などを格納する。

制御部 76 は、受注者端末装置 15 内の各構成要素の処理を統括的に制御する。

署名検証部 77 は、例えば、受注者 33 の公開鍵 $K_{33,P}$ を用いて、受注者端末装置 15 が作成した署名情報の検証を行う。

【0025】

〔認証装置 50〕

図 4 に示すように、認証装置 50 は、受信部 81、送信部 82、暗号化部 83、復号部 84、記憶部 85、制御部 86、署名作成部 87 および課金処理部 88 を有する。

ここで、受信部 81 および送信部 82 が、第 1 の発明の送受信手段に対応し、記憶部 85 が第 1 の発明の記憶手段に対応し、署名作成部 87 が第 1 の発明の署名作成手段に対応している。

【0026】

受信部 81 は、ネットワークを介して発注者端末装置 11、受注者端末装置 15 および認証装置 51 から情報あるいは要求を受信する。

送信部 82 は、ネットワークを介して発注者端末装置 11、受注者端末装置 15 および認証装置 51 に情報あるいは要求を送信する。

暗号化部 83 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 84 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 85 は、例えば、発注者 31 がネットワーク銀行 40 と契約を行うと、例えば、発注者 31 に割り当てられた秘密鍵 $K_{31,S}$ に対応する公開鍵 $K_{33,P}$ などを格納する。

制御部 86 は、認証装置 50 内の各構成要素の処理を統括的に制御する。

署名作成部 87 は、ネットワーク銀行 40 の秘密鍵 $K_{40,S}$ を用いて署名情報の作成を行う。

課金処理部 88 は、発注者 31 による取引に関する認証に対しての課金処理を行い、認証装置 51 との間で、前記取引に関する認証に対して行う課金の割合を決定するための処理を行う。

認証装置 50 の各構成要素の詳細な処理については、後述する動作例で記載する。

【 0 0 2 7 】

図 5 に示すように、認証装置 5 1 は、受信部 9 1、送信部 9 2、暗号化部 9 3、復号部 9 4、記憶部 9 5、制御部 9 6、署名作成部 9 7 および課金処理部 9 8 を有する。

受信部 9 1 は、ネットワークを介して受注者端末装置 1 5 および認証装置 5 0 から情報あるいは要求を受信する。

送信部 9 2 は、ネットワークを介して受注者端末装置 1 5 および認証装置 5 0 に情報あるいは要求を送信する。

暗号化部 9 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 9 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 9 5 は、受注者 3 3 がネットワーク銀行 4 1 と契約を行うと、例えば、受注者 3 3 に割り当てられた秘密鍵 $K_{33,S}$ に対応する公開鍵 $K_{33,P}$ などを格納する。

制御部 9 6 は、認証装置 5 1 内の各構成要素の処理を統括的に制御する。

署名作成部 9 7 は、ネットワーク銀行 4 1 の秘密鍵 $K_{41,S}$ を用いて署名情報の作成を行う。

課金処理部 9 8 は、受注者 3 3 による取引に関する認証に対しての課金処理を行い、認証装置 5 0 との間で、前記取引に関する認証に対して行う課金の割合を決定するための処理を行う。

【 0 0 2 8 】

以下、トランザクション認証システム 1 の動作例を説明する。

以下に示す動作例を開始する前提として、発注者 3 1 とネットワーク銀行 4 0 との間で所定の契約が結ばれ、ネットワーク銀行 4 0 は、発注者 3 1 に対して、個人キー情報 k_1 および個人 ID 情報 ID_1 を発行する。ネットワーク銀行 4 0 は、個人キー情報 k_1 および個人 ID 情報 ID_1 の対応表を図 4 に示す認証装置 5 0 の記憶部 8 5 に記憶する。ここで、個人キー情報 k_1 は、例えば、ネットワーク銀行 4 0 と契約した契約者（発注者 3 1）の契約番号などの個人情報を示す識別子である。また、個人 ID 情報 ID_1 は、発注者 3 1 の銀行口座番号などの課金に係わる情報を示す識別子である。

また、ネットワーク銀行40は、自らの秘密鍵 $K_{40,S}$ を図4に示す認証装置50の記憶部85に記憶すると共に、当該秘密鍵 $K_{40,S}$ に対応する公開鍵 $K_{40,P}$ を発注者端末装置11に送信する。発注者端末装置11は、公開鍵 $K_{40,P}$ を図2に示す記憶部65に記憶する。

【0029】

また、受注者33とネットワーク銀行41との間で所定の契約が結ばれ、ネットワーク銀行41は、受注者33に対して、個人キー情報Zおよび個人ID情報ID2を発行する。ネットワーク銀行41は、個人キー情報Zおよび個人ID情報ID2の対応表を図5に示す認証装置51の記憶部95に記憶する。

また、ネットワーク銀行41は、自らの秘密鍵 $K_{41,S}$ を図5に示す認証装置51の記憶部95に記憶すると共に、当該秘密鍵 $K_{41,S}$ に対応する公開鍵 $K_{41,P}$ を受注者端末装置15に送信する。受注者端末装置15は、公開鍵 $K_{41,P}$ を図3に示す記憶部75に記憶する。

【0030】

また、ネットワーク銀行40とネットワーク銀行41の間では、認証に関して相互乗り入れの契約がなされている。なお、認証装置50と認証装置51の間では、当該契約に基づいて、要求および情報の伝送が、公開鍵暗号方式あるいは共通鍵暗号方式を用いて行われる。

【0031】

図6は、トランザクション認証システム1の動作例を説明するための図である。

ステップST1：

発注者端末装置11は、図1に示す発注者31は、例えばネットワーク上の商店である受注者33に商品を発注する場合に、受注者33を特定する情報（例えば受注者33の名前）、発注する商品名および数量などを示す発注情報a1と、発注者31の個人キー情報k1と、発注者31の個人ID情報ID1とを、図示しない操作手段を操作して発注者端末装置11に入力する。なお、発注情報a1には、受注者33を特定する情報が含まれている。

次に、図2に示す発注者端末装置11の暗号化部63は、記憶部65から読み

出した所定の暗号鍵を用いて、発注情報 $a1$ と、個人キー情報 $k1$ および個人 ID 情報 $ID1$ を暗号化し、当該暗号化した情報を格納した認証要求 $inf1$ (本発明の第 1 の要求) を、送信部 62 からネットワークを介して、図 1 に示すネットワーク銀行 40 に送信する。

【 0 0 3 2 】

ステップ ST2 :

図 4 に示す認証装置 50 は、発注者端末装置 11 からの認証要求 $inf1$ を受信部 81 が受信すると、記憶部 85 から所定の暗号化鍵を読み出し、復号部 84 において、当該暗号鍵を用いて認証要求 $inf1$ を復号する。

次に、認証装置 50 は、制御部 86 の制御に基づいて、上記復号した認証要求 $inf1$ に格納された発注情報 $a1$ に含まれる受注者 33 を特定する情報 $b1$ を格納した要求 $inf2$ (本発明の第 2 の要求) を、記憶部 85 から読み出した所定の暗号鍵を用いて暗号化部 83 で暗号化した後に、受信部 81 からネットワークを介して認証装置 51 に送信する。

【 0 0 3 3 】

ステップ ST3 :

図 5 に示す認証装置 51 の制御部 96 は、認証装置 50 からの要求 $inf2$ を受信部 91 が受信すると、記憶部 95 から読み出した所定の暗号鍵を用いて復号部 94 において当該要求 $inf2$ を復号する。

次に、署名作成部 97 は、当該復号された要求 $inf2$ に格納された受注者 33 を特定する情報 $b1$ に対応する受注者 33 の公開鍵 $K_{33,p}$ を記憶部 85 から読み出し、当該公開鍵 $K_{33,p}$ について、記憶部 85 から読み出した自らの秘密鍵 $K_{41,s}$ を用いて自らの認証結果を示す署名情報 $Au-B$ (本発明の第 1 の署名情報) を作成する。

次に、暗号化部 93 は、受注者 33 の公開鍵 $K_{33,p}$ および署名情報 $Au-B$ を格納した応答 $inf3$ を、記憶部 95 から読み出した所定の暗号鍵を用いて暗号化した後に、送信部 92 から、ネットワークを介して認証装置 50 に送信する。

【 0 0 3 4 】

ステップ S T 4 :

図 4 に示す認証装置 5 0 の復号部 8 4 は、認証装置 5 1 からの応答 $inf 3$ を受信部 8 1 が受信すると、記憶部 8 5 から読み出した所定の暗号鍵を用いて、応答 $inf 3$ を復号する。

次に、署名作成部 8 7 は、ステップ S T 2 で復号した要求 $inf 1$ に格納された発注情報 $a 1$ および個人キー情報 $k 1$ を格納した情報 $inf 1'$ と、上記復号された応答 $inf 3$ に格納された署名情報 $Au-B$ と、記憶部 8 5 から読み出した自らの公開鍵 $K_{40,P}$ について、記憶部 8 5 から読み出した自らの秘密鍵 $K_{40,S}$ を用いて署名情報 $Au-A 1$ を作成する。

次に、制御部 8 6 は、情報 $inf 1'$ と、署名情報 $Au-B$ と、自らの公開鍵 $K_{40,P}$ と、上記生成した署名情報 $Au-A 1$ とを格納した要求 $inf 4$ (本発明の第 3 の要求) を生成する。

次に、暗号化部 8 3 は、ステップ S T 4 で認証装置 5 1 から受信した受注者 3 の公開鍵 $K_{33,P}$ を用いて、上記生成した要求 $inf 4$ を暗号化した後に、送信部 8 2 から、ネットワークを介して受注者端末装置 1 5 に送信する。

【 0 0 3 5 】

ステップ S T 5 :

受注者端末装置 1 5 の復号部 7 4 は、認証装置 5 0 からの要求 $inf 4$ を受信部 7 1 が受信すると、記憶部 7 5 から読み出した自らの秘密鍵 $K_{33,S}$ を用いて、要求 $inf 4$ を復号する。

次に、受注者端末装置 1 5 の署名検証部 7 7 は、上記復号した要求 $inf 4$ に格納された署名情報 $Au-B$ を、記憶部 7 5 から読み出した認証装置 5 1 の公開鍵 $K_{41,P}$ を用いて検証する。また、署名情報検証部は、上記復号した要求 $inf 4$ に格納された認証装置 5 0 の公開鍵 $K_{40,P}$ を用いて、要求 $inf 4$ に格納された署名情報 $Au-A 1$ を検証する。

【 0 0 3 6 】

受注者端末装置 1 5 の制御部 7 6 は、署名検証部が上記検証の結果、署名情報 $Au-B$ 、 $Au-A 1$ の正当性が認証されると、要求 $inf 4$ に格納された情報 $inf 1'$ と、署名情報 $Au-B$ 、 $Au-A 1$ と、自らの個人キー情報 Z とを格

納した応答 $inf5$ （本発明の所定の応答）を生成する。

次に、受注者端末装置 15 の送信部 72 は、上記生成した応答 $inf5$ を、上記復号した要求 $inf4$ に格納された認証装置 50 の公開鍵 $K_{40,P}$ を用いて復号した後に、送信部 72 から、ネットワークを介して認証装置 50 に送信する。

受注者端末装置 15 によって、署名情報 $Au-B$ 、 $Au-A1$ の正当性が認証されると、受注者 33 は、例えば、要求 $Inf4$ に格納された情報 $Inf1'$ 内の発注情報 $a1$ に基づいて、発注者 31 が発注した商品等を発注者 31 に発送したり、発注者 31 が注文したサービスを発注者 31 に提供する。

【0037】

ステップ ST6：

認証装置 50 の復号部 84 は、受注者端末装置 15 からの応答 $inf5$ を受信部 81 が受信すると、記憶部 85 から読み出した自らの秘密鍵 $K_{40,S}$ を用いて、 $inf5$ を復号し、要求 $inf1$ に格納された発注情報 $a1$ と、当該復号された $inf5$ に格納された受注者 33 の個人キー情報 Z とを用いて、所定の取り引き履歴情報を作成し、これを記憶部 85 に格納する。当該履歴情報は、ネットワーク銀行 40 が、発注者 31 に対して決済を行う際に用いられる。

また、認証装置 50 の署名作成部 87 は、ステップ ST2 で受信した要求 $inf1$ と、応答 $inf5$ に含まれる受注者 33 の個人キー情報 Z と、ステップ ST4 で作成した署名情報 $Au-A1$ について、自らの秘密鍵 $K_{40,S}$ を用いて自らの認証結果を示す署名情報 $Au-A2$ （本発明の第 2 の署名情報）を作成する。

次に、認証装置 50 の制御部 86 は、要求 $inf1$ と、個人キー情報 Z と、署名情報 $Au-A1$ と、署名情報 $Au-A2$ とを格納した応答 $inf6$ を作成する。

。

【0038】

次に、認証装置 50 の暗号化部 83 は、上記作成した応答 $inf6$ を、認証装置 50 から読み出した所定の暗号鍵を用いて暗号化した後に、送信部 82 から、ネットワークを介して発注者端末装置 11 に送信する。

発注者端末装置 11 では、受信した応答 $inf6$ を、図 2 示す記憶部 65 から読み出した所定の暗号鍵を用いて復号部 64 で復号する。

次に、発注者端末装置 1 1 の署名検証部 6 6 は、当該復号した応答 $inf 6$ に格納された署名情報 $Au-A 1$ 、 $Au-A 2$ を、記憶部 6 5 から読み出したネットワーク銀行 4 0 の公開鍵 $K_{40,P}$ を用いて検証することで、受注者端末装置 1 5 との間の当該取り引きが正当に認証されたことを確認する。

【 0 0 3 9 】

以上説明したように、トランザクション認証システム 1 によれば、認証装置 5 0 から認証装置 5 1 へは、発注者 3 1 の個人キー情報 $k 1$ および個人 ID 情報 $ID 1$ を送信しないことから、発注者 3 1 の個人情報が、発注者 3 1 が契約していない他のネットワーク銀行 4 1 に漏れることを回避できる。

【 0 0 4 0 】

また、トランザクション認証システム 1 によれば、認証装置 5 0 が、認証装置 5 1 から受けた受注者 3 3 の公開鍵 $K_{33,P}$ および署名情報 $Au-B$ を用いて、受注者 3 3 の受注者端末装置 1 5 との間で直接通信を行うことで、当該取り引きの履歴を認証装置 5 0 に格納できる。

また、トランザクション認証システム 1 によれば、受注者 3 3 は、自らの契約した認証装置 5 0 の署名情報 $Au-B$ を検証することで、当該取り引きの正当性を確認できる。

また、トランザクション認証システム 1 によれば、認証装置 5 0 と 5 1 との間では、図 6 に示す要求 $inf 2$ および $inf 3$ を伝送するだけで、発注者 3 1 と受注者 3 3 との間の取り引きを認証でき、認証装置 5 0 と 5 1 との間の通信量を小さくできる。

【 0 0 4 1 】

また、トランザクション認証システム 1 によれば、図 4 に示す認証装置 5 0 の課金処理部 8 8 と、図 5 に示す認証装置 5 1 の課金処理部 9 8 との間で通信を行うことで、発注者 3 1 と受注者 3 3 との間の取り引きに関する認証に対して行う課金の割合を柔軟に決定できる。

【 0 0 4 2 】

上述したように、トランザクション認証システム 1 によれば、異なる認証機関と契約をしている複数の取り引き者の間の取り引きに関する認証を、高い信頼性

で、しかも効率的に行うことができる。その結果、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などを費用を低額にでき、電子商取引をさらに普及させることが可能になる。

【 0 0 4 3 】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、ネットワーク銀行 4 0、4 1 が、それぞれ認証装置 5 0、5 1 を用いて、トランザクション（取り引き）の認証業務を行う場合を例示したが、ネットワーク銀行 4 0、4 1 とは別の機関が、認証装置 5 0、5 1 を用いてトランザクションの認証業務を行うようにしてもよい。

【 0 0 4 4 】

また、上述した実施形態では、発注者 3 1 が契約したネットワーク銀行 4 0 の認証装置 5 0 と、受注者 3 3 が契約したネットワーク銀行 4 1 の認証装置 5 1 との間で連携して認証処理を行う場合を例示したが、3 人以上の取り引き者がそれぞれ異なる認証機関と契約を行っている場合に、3 以上の認証装置間で連携して認証処理を行う場合にも、本発明は適用可能である。

【 0 0 4 5 】

また、上述した実施形態では、図 6 に示すステップ S T 1 のように、暗号化された発注情報 a 1 と、個人キー情報 k 1 および個人 I D 情報 I D 1 とを含む認証要求 I n f 1 を、発注者端末装置 1 1 から認証装置 5 0 に送信する場合を例示したが、発注情報 a 1 および個人キー情報 k 1 を含む認証要求 I n f 1 を、発注者端末装置 1 1 から認証装置 5 0 に送信してもよい。このようにすれば、課金に係わる情報である個人 I D 情報 I D 1 はネットワークを介して伝送されないため、ネットワーク上で個人 I D 情報 I D 1 が不正に取得され、悪用されることを回避できる。

【 0 0 4 6 】

また、本発明では、例えば、認証装置 5 0 から受注者端末装置 1 5 に、署名情報 A u - A 2（本発明の第 2 の署名情報）を送信するようにしてもよい。

【 0 0 4 7 】

【発明の効果】

以上説明したように、本発明によれば、例えば異なる認証機関と契約した複数の取引引き者間での取引引きの認証を、取引引き者の個人情報を他の認証機関に提供することなく、高い信頼性で行うことができる認証装置、認証システムおよびその方法を提供できる。

【図面の簡単な説明】

【図 1】

図 1 は、本発明の実施形態のトランザクション認証システムの全体構成図である。

【図 2】

図 2 は、図 1 に示す発注者端末装置の構成図である。

【図 3】

図 3 は、図 1 に示す受注者端末装置の構成図である。

【図 4】

図 4 は、図 1 に示す認証装置 (A) の構成図である。

【図 5】

図 5 は、図 1 に示す認証装置 (B) の構成図である。

【図 6】

図 6 は、図 1 に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

【符号の説明】

1 … トランザクション認証システム、11 … 発注者端末装置、15 … 受注者端末装置、31 … 発注者、33 … 受注者、40, 41 … ネットワーク銀行、50, 51 … 認証装置、61, 71, 81, 91 … 受信部、62, 72, 82, 92 … 送信部、63, 73, 83, 93 … 暗号化部、64, 74, 84, 94 … 復号部、65, 75, 85, 95 … 記憶部、66, 76, 86, 96 … 制御部、67, 77 … 署名検証部、87, 97 … 署名作成部、88, 98 … 課金処理部

a1 … 発注情報、k1 … 発注者 31 の個人キー情報 k1、ID1 … 発注者 31 の個人 ID 情報、b1 … 受注者を特定する情報、Au-B … 認証装置 51 の署名情報、Au-A1, Au-A2 … 認証装置 50 の署名情報、Z … 受注者の個人

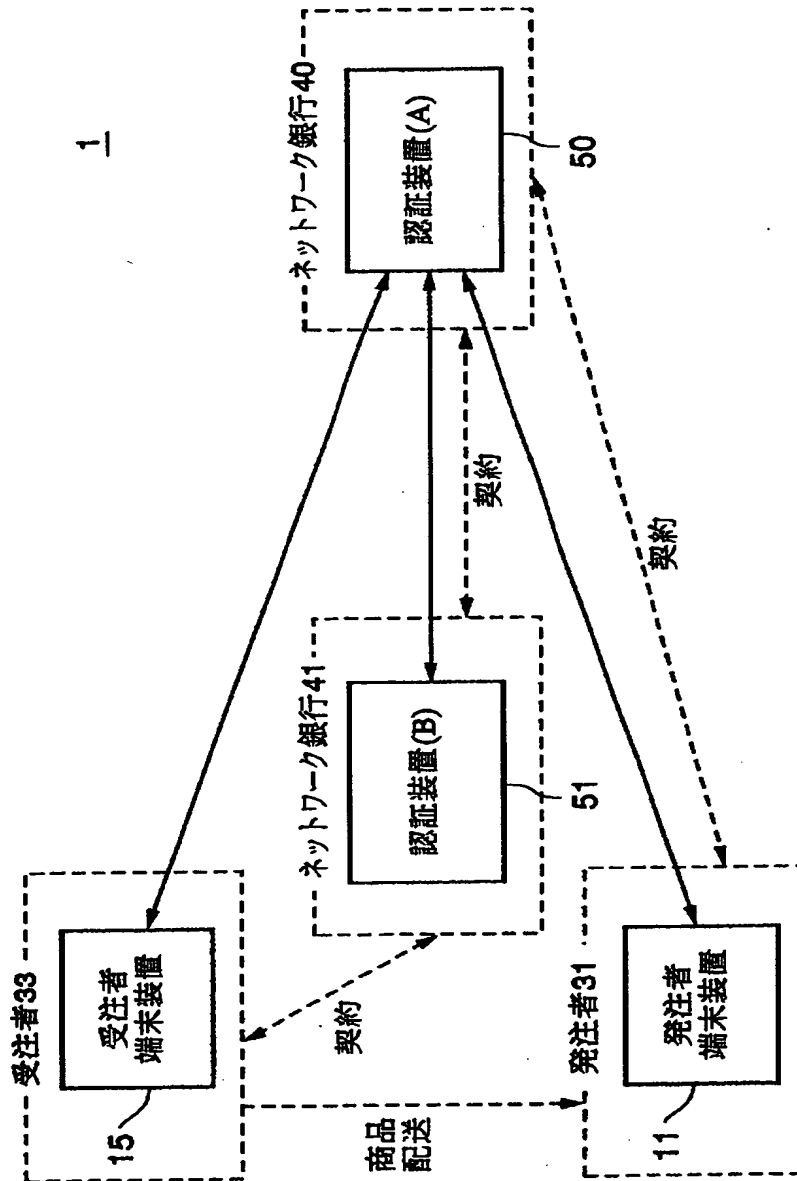
特 2 0 0 0 - 2 0 9 6 7 4

キ一情報

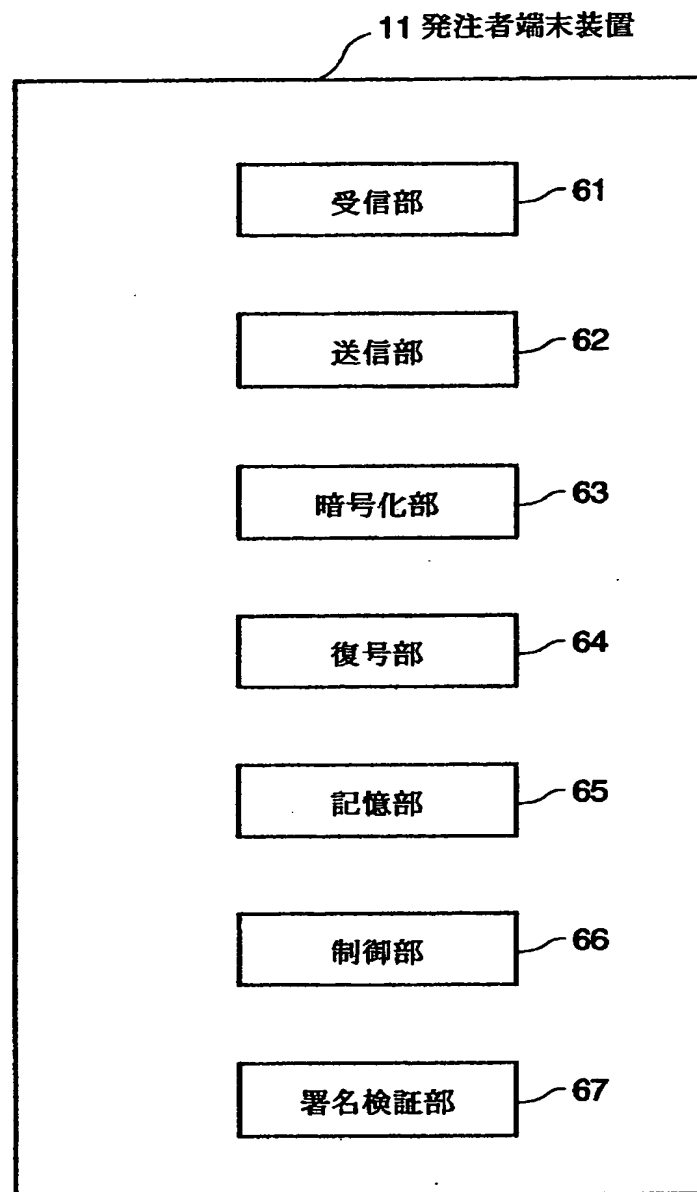
【書類名】

図面

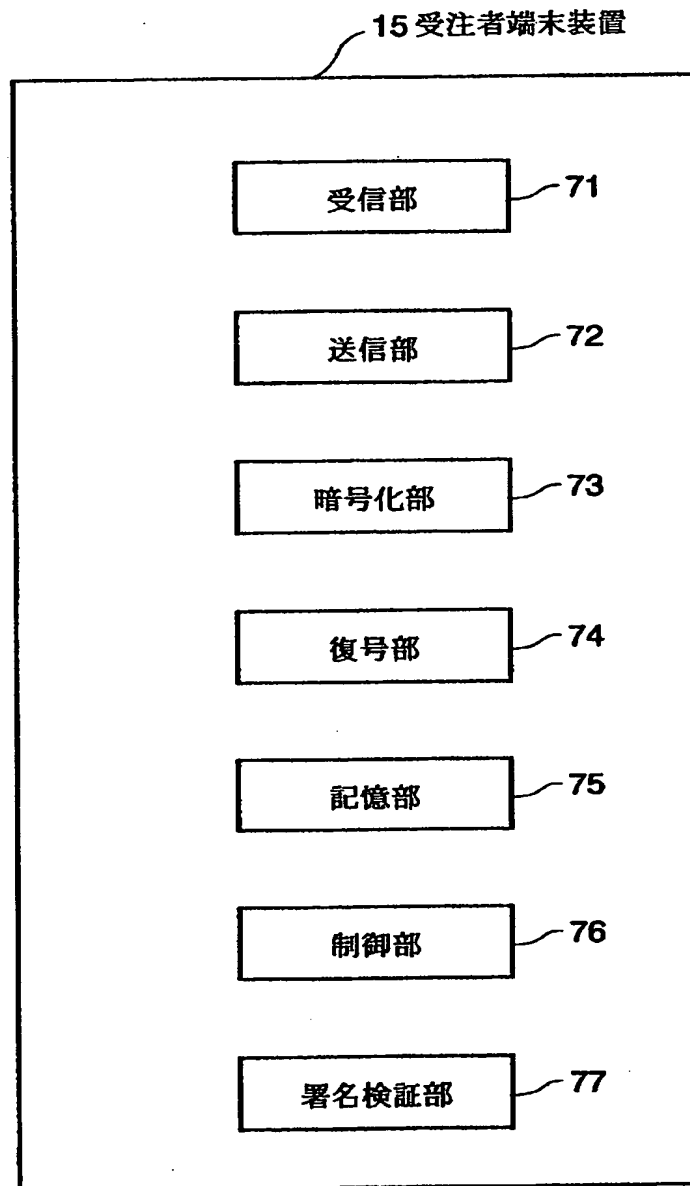
【図1】



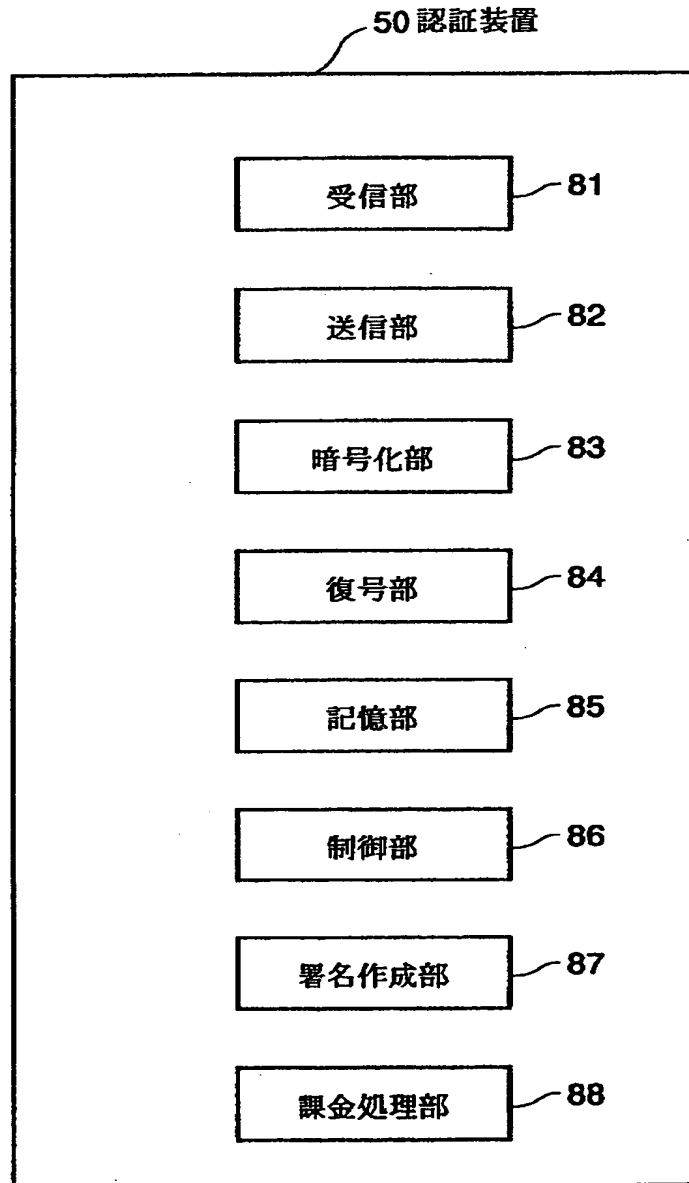
【図 2】



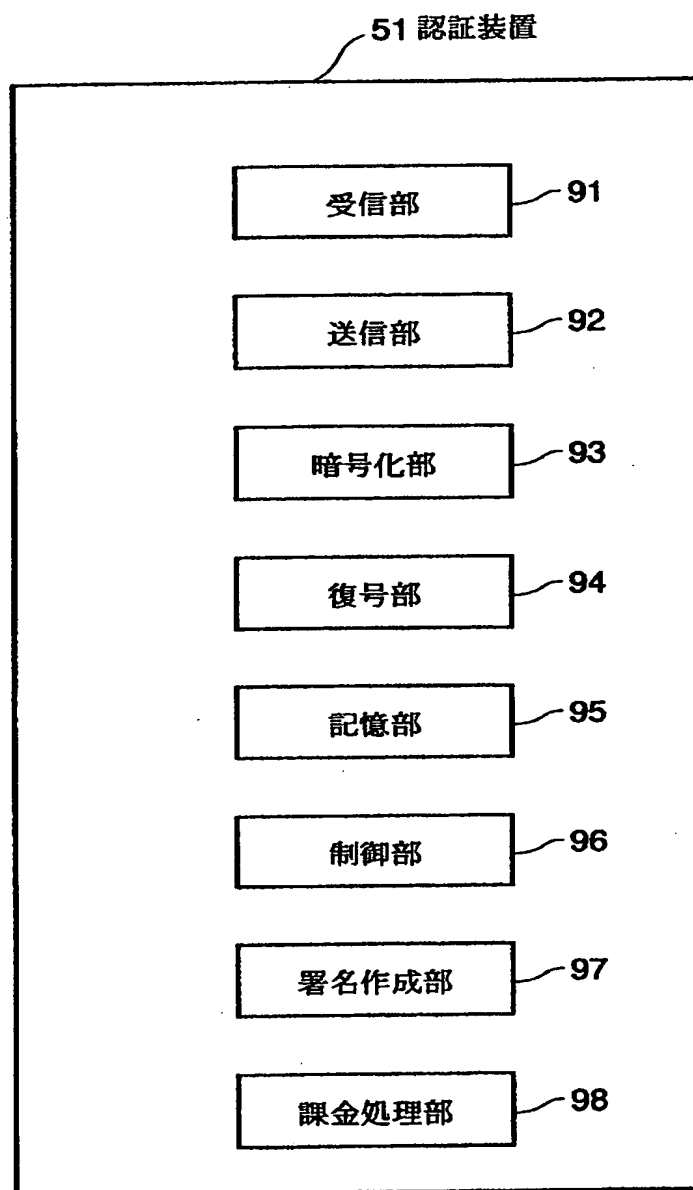
【図 3】



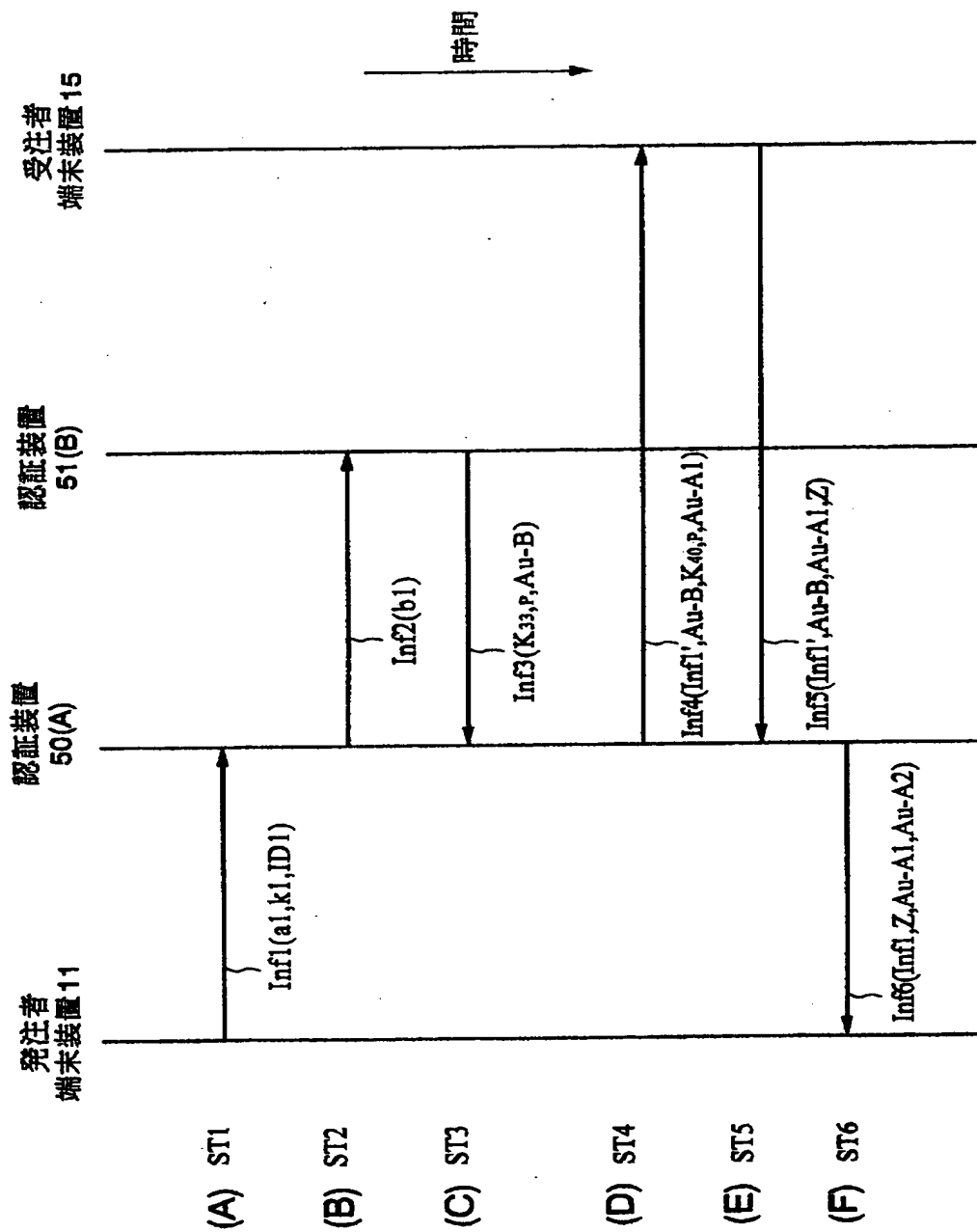
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 異なる認証機関と契約した利用者相互間の取り引きの認証を、利用者の個人情報を他の認証機関に提供することなく、高い信頼性で行うことができる認証装置を提供する。

【解決手段】 発注情報と受注者 3 3 を特定する情報とを含む要求が発注者端末装置 1 1 から認証装置 5 0 に出されると、認証装置 5 0 から 5 1 に対して受注者 3 3 を特定する情報が送信され、認証装置 5 0 が 5 1 から所定の署名情報を受信する。認証装置 5 0 は、受注者端末装置 1 5 に発注情報と上記署名情報とを送信し、受注者端末装置 1 5 から個人キーを受信する。そして、認証装置 5 0 は、当該取り引きの履歴を記憶すると共に発注者端末装置 1 1 に所定の署名情報を送信する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社